



Received & Inspected

July 12, 2010

JUL 14 2010

FCC Mail Room

Commission's Secretary
Office of the Secretary
Federal Communications Commission
445 12th St., SW., Room TW-A325
Washington, DC 20554

RE: Comments on PS Docket No. 10-93 and/or rulemaking FCC 10-63

Dear Commission's Secretary,

I am writing on behalf of (ISC)², a not-for-profit organization dedicated to improving the skills and capabilities of the global information security workforce through professional education and certification and public awareness. (ISC)² has over 70,000 certified information security professionals in 135 countries. We sincerely appreciate your continuing interest in the increasing security of the nation's broadband infrastructure and the promotion of vigilant cyber security public and communications providers.

The American National Standards Institute (ANSI) is a private non-profit organization whose mission is to enhance U.S. global competitiveness and the American quality of life by promoting, facilitating and safeguarding the integrity of the voluntary standardization and conformity assessment systems. ANSI represents the interests of more than 125,000 companies and 3.5 million professionals worldwide. The institute is the official U.S. representative to the International Organization for Standardization (ISO) and, via the U.S. National Committee, the International Electrotechnical Commission (IEC) and is a US. Representative to the International Accreditation Forum (IAF). Accordingly, ANSI's comments will be referenced within the document.

We sincerely appreciate your continuing interest in the increasing security of the nation's broadband infrastructure and the promotion of vigilant cyber security public and communications providers. A voluntary or mandatory program to develop awareness for both the need to improve cyber security practices and develop approaches to practicably make such improvements is an important public policy goal.

We believe that through a well-crafted public-private partnership such a program can:

- (1) Increase the security of the nation's broadband infrastructure;
- (2) Promote a culture of more vigilant cyber security among participants in the market for communications services; and
- (3) Offer end users more complete information about their communication service providers' cyber security practices.

No. of Copies rec'd 0
List A B C D E

We would also like to commend you on reviewing the 2009 Global State of Information Security study reported that showed that budgets for information security initiatives are being reduced at a time of heightened attacks and the 2008 Data Breach Investigation Report which concluded that 87% of cyber breaches could have been avoided if reasonable security controls had been in place which would include properly credentialed professionals responsible for assuring the necessary security controls needed are properly implemented. We also commend the Commission on its actions in supporting the Network Reliability and Interoperability Council (NRIC) best practices for securing computers and other software-controlled network equipment to industry.

We would like to respond to the issue that a voluntary incentives-based certification program should be developed in which participating communications service providers will receive network security assessments by approved, private-sector auditors, who will examine those provider's adherence to stringent cyber security practices that have been developed, through consensus, by a broad-based public-private sector partnership and whether this program should be voluntary or mandatory;

In our opinion, any incentive would have to carry the cost of assessment as well as the costs of controls to be put in place. The anticipated cost may be significant so incentives such as the ability to proclaim marketing advantage for a service provider would not be sufficient incentive. A strategy should be developed to incorporate security into broadband suppliers' business model. Our suggestion would be to do take the following steps:

1. Convene a high level group of security experts to review the industry and develop a list of best practices that are most applicable to broadband service providers based upon threat and risk to the public and the companies. There are several attractive methodologies that may be used in the initial evaluation including: ISO/IEC 27001 or the less complex National Security Agency Information Assessment Methodology. In accordance with OMB Memorandum 10-15, a SAS70 review may also be considered.
2. The first iteration of best practices should be based on the following principle of where the most benefit is accrued from fixing the greatest threat and at reasonable cost. The concept of risk based assessment should be the guiding principle.
3. A mandatory program may be necessary if the results are to have improved security for nationwide broadband services. As indicated in your report, voluntary programs that have been attempted in the past have had mixed results.

Those providers whose networks successfully complete the assessment may then market their networks as complying with stringent FCC network security requirements. This increased recognition should provide more business opportunities because of the increased confidence in the security of the services provided.

On the issue for comment to offset the administrative costs associated with the voluntary certification program, should the commission collect fees from those communications

service providers that decide to participate? If so, how should such fees be determined and collected? Would the resultant costs outweigh the program's value to participants?

A government run certification program is likely to be quite costly to administer at an organizational level so fees would have to be extremely high to cover costs. Some of the existing certification bodies in the private sector have the infrastructure in place to offer such a program and may be able to establish a reasonable fee. For this reason, we believe it would be best to have a non-profit entity manage a certification program with the appropriate government involvement in a cost effective manner.

The following comments are provided on the four possible security objectives that are proposed as the starting point of the security regime: *(1) Secure equipment management; (2) updating software; (3) intrusion prevention and detection; and (4) intrusion analysis and response. Are these sufficient as the initial set?*

These are part of a holistic solution so the broadband industry should institute governance to meet the overall security objectives. Additionally, service providers should consider how to provide services if an incident occurs and what the educational needs are of its user groups. Broadband service providers currently have user agreements which are embedded in policy so policy should also be considered in review. By focusing on the technical end point solution, an overall strategy to meet and manage security will be missing. A risk management approach by broadband suppliers should be strongly considered to meet the overall goal of governance.

Should the private-sector bodies involved in this certification program have extensive responsibilities in this program, or should the commission retain primary responsibility for the maintenance and administration of the proposed program?

Currently, certification bodies are managed in the private-sector. The FCC does not have the experience to perform the task of certification at this time so it would be sensible to use the private sector for this task. The not-for-profit certification organizations have a great deal of experience in applying the best practices in information security, have the certification policies and procedures that are applicable and the resources to assume this responsibility. The Commission should have the oversight of this program, but not be involved in operations and day to day management of the certification program(s).

The Commission also seeks comment on whether ANSI accreditation procedures should formally apply to the certification authority in regard to the accreditation of standard developers. If so, should it be the Organization Method or the Standards Committee Method that applies?

(ISC)² references ANSI's letter and is in agreement for the next seven paragraphs.

By way of background, with respect to standards development, ANSI accredits the procedures of standards developers in accordance with the due process requirements established in the *ANSI Essential Requirements: Due process requirements for American National Standards (ANSI Essential Requirements.)* ANSI's requirements mirror those

contained in the definition of “voluntary consensus standards” as set-forth in OMB Circular A-119. Accreditation by ANSI means that the procedures used by a standards developer in connection with the development of evidence of consensus in support of a draft standard’s approval as an American National Standard (ANS) satisfy ANSI’s procedural requirements. ANSI does not distinguish among methods of standards development, e.g., organization versus committee. All ANSI-Accredited Standards Developers are required to satisfy the same criteria and are subject to the same neutral, third-party ANSI oversight. Moreover, one cannot meaningfully distinguish among methods as some standards development organizations implement their consensus processes via committees, while others employ different, yet equivalent, models.

The American National Standards process and ANSI’s accreditation of standards developers exemplifies a robust and effective public-private partnership that benefits our Nation and minimizes public sector costs. The benefits of ANSI’s standards developer accreditation program and of the approval of standards as American National Standards include credibility, process integrity, public recognition and other advantages that are summarized in the ANS Value brochure available at www.ansi.org/ansvalue. ANSI-accredited standards developing organizations - and the experts that populate the consensus bodies of these groups as voting members as well as the public that contributes to the standards by commenting on them - serve an important public interest function in devising American National Standards. The public interest is both served and protected if the standards development process is accredited by ANSI as meeting the Institute’s requirements for openness, balance, consensus, appeals and other due process safeguards.

There are some 223 ANSI-Accredited Standards Developers working in a broad range of areas of standardization. A complete list is available at www.ansi.org/asd. A number of ANSI-Accredited Standards Developers, including IEEE, INCITS, ATIS, NEMA, SCTE, TIA, CEA and others are already involved as leaders in relevant standardization activities. We encourage FCC reliance on ANSI and the American National Standards process, which provide all interested parties – government, industry, consumers and other materially affected interests - with a neutral venue to come together and work towards common agreements. As the coordinator of the U.S. voluntary consensus standards system, ANSI serves as a facilitator, providing an infrastructure and process by which proposed American National Standards (ANSs) may be vetted. ANSI’s role is to safeguard the integrity of this system, which by design, is based on a private-public partnership that is driven by the needs of the range of markets in this country and by the public interest.

The ANSI standard development process would seem to be appropriate for this program. Standards Developer Organization(s) should be identified. Compliance with ANSI essential requirements that ensures public-private participation is important. The Commission and related governmental agencies along with the private sector should participate in the development of the standard. This will result in an American National

Standard that has industry acceptance and very specific comprehensive requirements that ensures network operators successfully perform their operations.

These requirements should cover different types of cyber security providers. The standard's development committee should determine the certification interval and not leave it to individual certifying agencies to ensure consistency or this type of information can be placed in a separate normative document that will guide the specific certification policies and procedures. The later is preferable.

In addition to ANSI's Standard Development Organization accreditation program, ANSI accredits certification bodies that certify systems, products and personnel... Accreditation of certification bodies further assures that they are properly implementing their policies and procedures; that the necessary security controls are in place; and that the people responsible possess the competencies needed to ensure that controls are in place and functioning correctly.

The standard most appropriate for this accreditation process -- and implemented by ANSI - is ISO/IEC 17011 -- *Conformity Assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies*. Additionally, it appears that one or more personnel certification bodies should be identified to certify the auditors of the communication service providers. The auditors who perform this assessment under a national standard should be certified in accordance with ANSI/ISO/IEC 17024 -- *Conformity Assessment -- General requirements for bodies operating certification of persons*. These auditors must be certified minimally in the four identified knowledge domains (a) security equipment management (b) updating software (c) intrusion prevention and detection (d) intrusion analysis and response. Auditors would need to be experts in the requirements of broadband service providers as well as the auditing process.

On issue for comment to the Commission *on whether it would be necessary to establish: (1) What portion of the applicable assessment criteria a provider must pass in order to successfully complete the assessment; (2) what percentage of a provider's operations the auditors must examine for compliance with applicable security criteria; (3) whether any level of self-certification by providers will be permitted on any of the assessment criteria; and (4) whether a particular assessment will be an "examination engagement" or an "agreed upon procedures audit."*

(ISC)² references ANSI's letter and is in agreement with the next paragraphs.

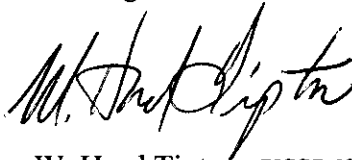
A program scheme should be developed based on a normative document crafted by the Commission in collaboration with the appropriate stakeholders regarding the desired and specific certification policy and procedures that would underpin this program. This would be in addition to the American National Standards that could be developed for this program or that may exist in some form. The normative document will assure consistency among certification bodies and provide the transparency that must exist for the broadband service providers to enable/ensure that the responsibility for

revoking/suspending certification and all related appeals options should be left to the certification bodies subject to accreditation requirements and applicable procedures, which would involve the Accreditation body operating within the program scheme with FCC participation.

Where the Commission seeks comment on how to improve education on cyber security issues. What actions, if any, can the Commission take to better educate end users, including consumers, businesses and government agencies about cyber security? Are there, for example, educational and/or outreach activities in which the Commission, either alone or with other stakeholders (e.g., Federal agencies, state and local governments, private industry) should engage to assist individuals in protecting their personal computers and other devices?

Consideration should be given to educational programs for K-12 to begin educating the next generation of broadband users. Professional societies/associations and community colleges should be encouraged to develop Certificate programs that meet ASTM E 2659, Standard Practice for Certificate Programs.

Best regards,

A handwritten signature in black ink, appearing to read "W. Hord Tipton". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

W. Hord Tipton, CISSP-ISSEP, CAP, CISA
Executive Director
(ISC)²